(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 November 2001 (08.11.2001)

PCT

(10) International Publication Number
WO 01/84517 A2

(51) International Patent Classification⁷: G07F 19/00

(21) International Application Number: PCT/US01/13814

(22) International Filing Date: 30 April 2001 (30.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/200,337 28 April 2000 (28.04.2000) US

(71) Applicant *(for all designated States except US)*: **EQUIFAX, INC.** [US/US]; 1550 Peachtree Street, N.W., Atlanta, GA 30309 (US).

(72) **Inventor; and**
(75) **Inventor/Applicant** *(for US only)*: **MALCONIAN, Michele** [US/US]; 4957 Orange Grove Way, Palm Harbor, FL 34684 (US).

(74) **Agent: PRATT, John, S.**; Kilpatrick Stockton LLP, Suite 2800, 1100 Peachtree Street, Atlanta, GA 30309-4530 (US).

(81) **Designated States** *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) **Designated States** *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/84517 A2

(54) **Title:** SYSTEM AND METHOD FOR SECURE NETWORK TRANSACTIONS

(57) **Abstract:** A comprehensive payment and security architecture presents an Internet or other consumer with the ability to pay for network transactions using authenticated check or other cash account, debit account, credit account and other payment options. A transaction server may authenticate the consumer's identity and verify the amount and type of payment, including to determine whether the transaction may be processed using the Automated Clearing House (ACH) system. Varying degrees in authentication score may result in the presentation of different payment options. Signatureless paper drafts may be generated for check-based transactions, depending on participating bank and other variables. Payment flexibility and transaction security are enhanced.

SYSTEM AND METHOD FOR SECURE NETWORK TRANSACTIONS

This application claims priority to U.S. Application Number 60/200,337 filed on April 28, 2000 entitled "**SYSTEM AND METHOD FOR SECURE NETWORK TRANSACTIONS.**"

FIELD OF THE INVENTION

The invention relates to the field of electronic commerce, and more particularly to a payment engine for networked transactions permitting a selection of check or other cash account, credit card account and other credit, debit or other payment options using authenticated payment channels.

BACKGROUND OF THE INVENTION

Business surveys in 1998 indicated that in the second half of 1996, 3.2 million households were making online purchases. That number doubled in the second half of 1997 where 7 million plus households were reported to be making online purchases. Spending in the year 2000 over the Internet is projected to be an average $99 per person, while total purchases over the Web in 2001 is estimated to total $228 billion. The portion that will be consumer to business is 11%. The portion that will be business to business is projected to be 89%. Clearly, the demand for business and consumer-to-business networked commerce is increasing significantly.

However, network payment techniques have not kept pace with this burgeoning demand. Third party credit card payments have become a default solution because of convenience. However, these payment networks have drawbacks. To merchants, every card transaction involves accepting a discount of approximately 2 to 5% in exchange for the credit card provider's services. To the consumer, privacy may be compromised by transmitting sensitive credit card or other information for storage on vendor and other servers. Other drawbacks exist.

SUMMARY OF THE INVENTION

The invention overcoming these and other problems in the art in one regard relates to a network payment solution for the Internet and other network environments for consumer, business, and other transactions.

Briefly described the present invention provides systems and methods for a merchant to authenticate a consumer and to accept on-line payments from the consumer. The system authenticates the consumer and creates a certainty score for this consumer. This certainty score may affect the level of on-line credit granted by the merchant. The on-line payment system utilizes risk parameters to determine whether to authorizes an on-line payment request.

The invention in one embodiment may deploy a suite of transaction services including secure authentication, point of sale retail promotions, check warranty and check verification/self-risk functions, Automated Clearing House (ACH) settlement, collection services and complete credit card services for the Internet and other use. The invention in another regard may support transaction settlement, private label card issuance and processing and other affinity or marketing programs.

The invention may support initiation, verification, and payment completion through a variety of networked or non-networked channels, such as virtual storefronts or mail/telephone order. The invention may be implemented in a modular fashion to allow the transaction services to be unbundled in order to meet specific client needs. The invention furthermore allows checks to be authorized by telephone or by fax, and settled electronically.

Using the invention, consumers may authenticate their identity and be assured a secure Internet shopping experience, while minimizing risk on check and credit card transactions to them and to vendors, payors, and others. The invention may record authentication information on a relational database along with the consumer's driver's license, state, date of birth and full MICR information, which may become part of a new comprehensive consumer database.

It is consequently one object of the invention to provide an electronic payment system capable of complete transaction support, including to provide electronic retail "e-tailing" check verification, self-risk, or warranty services.

It is another object of the invention to provide an electronic payment system capable of authenticating the identity of consumers at the point of sale.

It is another object of the invention to provide an electronic payment system capable of originating Automated Clearing House Association (ACH) transactions for settlement of US Checks and Canadian Checks.

It is another object of the invention to provide an electronic payment system capable of identifying "non-ACHable" items (items that cannot be handled by ACH transactions) at the time of authorization where possible and create paper drafts.

It is another object of the invention to provide an electronic payment system capable of producing check drafts for items returned non-ACHable.

It is another object of the invention to provide an electronic payment system capable of providing collections for self-risk items.

It is another object of the invention to provide an electronic payment system capable of providing card authorization and settlement.

It is: another object of the invention to provide an electronic payment system capable of providing private label card services.

It is another object of the invention to provide an electronic payment system capable of providing online and offline Decision Power Retail options to clients with private label cards.

BRIEF DESCRIPTION OF DRAWINGS

The invention will be described with reference to the accompanying drawings, in which like elements are referenced by like numerals.

Figure 1 illustrates payment architecture according to one embodiment of the invention.

Figure 2 illustrates a flowchart of payment processing according to an embodiment of the invention.

Figure 3 illustrates a user process according to another embodiment of the present invention.

Figure 4 illustrates an authentication process according to an embodiment of the present invention.

Figure 5 illustrates a payment process according to an embodiment of the present invention.

DATAILED DESCRIPTION OF PREFERRED EMBODIMENTS

In a transaction and payment architecture that supports secure network transactions according to the invention illustrated in Figure 1, a consumer operating a client device 102 may access a transaction vendor 106 via a communications link 104 to investigate or execute an electronic transaction, such as a purchase, rental or other transaction over the Internet or other network.

The transaction vendor 106 may be an electronic retailer such as Amazon.com™, a catalog retailer such as Service Merchandize™, or a traditional retailer with a storefront who has a web presence on the Internet. The transaction vendor 106 generally subscribes to a secure network transaction service from a service provider. However, the transaction vendor 106 can also be the service provider.

The client device 102 may be or include, for instance, a personal computer running the Microsoft Windows™ 95, 98, Millenium™, or 2000, Windows CE™, PalmOS™, Unix, Linux, Solaris™, OS/2™, BeOS™, MacOS™ or other operating system or platform. Client device 102 may also be or include a network-enabled appliance such as a WebTV™ unit, radio-enabled Palm™ Pilot or similar unit, a set-top box, a networkable game-playing console such as Sony Playstation™ or Sega Dreamcast™, a browser-equipped cellular telephone, or other TCP/IP client or other device.

The communications link 104 over which the client device 102 communicates with the transaction vendor 106 may be, include or interface to any one or more of, for instance, the Internet, an intranet, a PAN (Personal Area Network), a LAN (Local Area Network), a WAN (Wide Area Network) or a MAN (Metropolitan Area Network), a frame relay connection, an Advanced Intelligent Network (AIN) connection, a synchronous optical network (SONET) connection, a digital T1, T3, E1 or E3 line, Digital Data Service (DDS) connection, DSL (Digital Subscriber Line) connection, an Ethernet connection, an ISDN (Integrated Services Digital network) line, a dial-up port such as a V.90, V.34 or V.24bis analog modem connection, a cable modem, an ATM (Asynchronous Transfer Mode) connection, or FDDI (Fiber Distributed Data Interface) or CDDI (Copper Distributed Data Interface) connections.

Communications link 104 may furthermore be, include or interface to any one or more of a WAP (Wireless Application Protocol) link, a GPRS (General Packet Radio Service) link, a GSM (Global System for Mobil Communication) link, a CDMA (Code Division Multiple Access) or TDMA (Time Division Multiple Access) link such as a cellular phone channel, a GPS (Global Positioning System) link, CDPD (cellular digital packet data), a RIM (Research in Motion, Limited) duplex pagingtype device, a Bluetooth radio link, or an IEEE 802.11-based radio frequency link. Communications link 104 may yet further be, include or interface to any one or more of an RS-232 serial connection an IEEE-1394 (Firewire) connection, a Fibre Channel connection, an IrDA, (infrared) port, a SCSI (Small Computer Systems Interface) connection a USB (Universal Serial Bus) connection or other wired or wireless, digital or analog interface or connection. Other communications links described herein may be or include similar communications resources.

In the transaction environment of the invention, once the consumer on client device 102 has finished shopping they may click on "check out" via the user interface 150 and then selects a payment type, e.g., "Pay by Check." The transaction vendor 106 may then communicate the transaction to a transaction server 110 over a communication link 108. The transaction server 110 and other servers described herein may be or include, for instance, a workstation running the Microsoft Windows NT™, Windows™ 2000, Unix, Linux, Xenix, IBM AIX™, Hewlett-Packard UX™, Novell Netware™, Sun Microsystems Solaris™, OS/2™, BeOS™, Mach, Apache, OpenStep™ or other operating system or platform.

If the consumer operating the client device 102 has not been through an authentication process, an interactive authentication process may begin. The authentication process may be handled by a third party vendor from who the transaction vendor 106 subscribes the authentication service.

The consumer may apply for authentication via the transaction vendor 106 which links to an authentication server 114 via the transaction server 110 and communications link 112. Consumer information entered on a web site or other data port of transaction vendor 106, such as name, address, telephone SSN, driver's license number etc., is then communicated to authentication server 114.

The consumer may be prompted on user interface 150 to enter additional information not processed by the transaction vendor 106. If the captured or entered data does not meet the initial formatting or other criteria applied by authentication server 114, a message may be returned to the consumer requesting the data in question, to be corrected and resubmitted.

The authentication process may be a multi-step process. The authentication process asks initially some basic information from the user. If the user provides the correct basic information, the authentication process then proceeds to ask for additional information normally not easily known by third parties. The additional information asked may derive from the user's credit file history or other sources.

Once the consumer completes the first step of the authentication verification process, the information is forwarded to a further verification step, i.e. the second step of the authentication process. In that step, the information may be compared to external databases such as the commercial credit databases from a credit-reporting agency such as Equifax Inc., or telephone number or driver's license databases. Matching algorithms may be used to determine the quality or degree of the match and a score indicating that degree may be generated. The scoring, authentication and related algorithms may be or include those described in co-pending U.S. Patent Application Serial Nos. 09/315,128 filed May 20th, 1999 entitled "System and Method For Authentication of Network Users"; 09/315,129 filed May 20, 1999 entitled "System and Method For Authentication of Network Users And Issuing a Digital Certificate"; and 09/315,130 filed May 20, 1999 entitled "System and Method For Authentication of Network Users With Preprocessing", each assigned to the same assignee as this application and incorporated by reference herein, or others.

A further stage of verification may be employed, in which an interactive query may be presented to the consumer to answer multiple choice questions non-wallet data. Those questions may be weighted, and the responses scored. A composite scoring algorithm may then be used, based upon the scores from the ID compare, interactive query or other stages to create an overall certainty score, for instance on a scale of 1-100. If the certainty score is low enough, the authentication may be denied.

At the end of the authentication process, the authentication server 114 provides the user with an identification code (ID) and a password.

Once the consumer satisfies the authentication threshold set by transaction vendor 106 or otherwise, the consumer may be prompted to create a login/password. The certainty score may be stored via the login/password in consumer database 122, and other data fields such as driver's license number, full magnetic ink character recognition (MICR) number (the bank number and the bank account number that appear on the lower corner of a check), date of birth, positive/negative check writing history, etc. may be recorded in that media or otherwise.

If the consumer has been validated via the authentication server 114 and related processes, the consumer may enter their login/password and the transaction server 110 may validate the login information against the consumer database. If the login/password do not match the information in consumer database 122, then the consumer may be given a predetermined number of chances, such as 1 additional opportunity to correct and enter the information. If the consumer cannot enter the correct information, the consumer may be instructed to contact an administrator of transaction through the transaction server 110 or other party via preferably email for assistance, through a hot link, or alternatively to go through the authentication process once again depending on implementation.

The consumer's resulting certainty score, either newly created during the interactive session or previously issued, retrieved from consumer database 122, is compared to a threshold score, which may be established by transaction vendor 106 or otherwise. A vendor may employ one threshold for check transactions and a separate threshold for card transactions. Alternately, the service provider, who validates payment transactions, may establish a common threshold for all transaction using a same payment type.

If the certainty score meets the threshold for the selected payment type set by either the transaction vendor 106 or the service provider, then the consumer is prompted to enter the remaining payment information required for authorization. If the certainty score does not meet the threshold for the payment type for the transaction vendor 106, but the score is high enough for an alternative payment type, then only those alternative options may be displayed and the consumer may choose one of those options.

If the consumer's certainty score meets neither threshold, the service provider may deny the authentication, and the consumer may be instructed on how to obtain a disclosure via the Internet, phone or mail. Manual updates to consumer database 122 and other resources may preferably be allowed to ensure that files are accurate. For example, if the consumer provides the appropriate documentation offline, a score would then be generated and the consumer database 122 would be updated for future use.

In a practice of the invention, if the consumer wishes to pay by check or other cash-based instrument, then the necessary consumer and sale information may be accepted by the authorization system of the invention. The invention, using risk management technologies, may determine whether the transaction is approved or declined for that type of fulfillment.

The risk management technologies may employ statistical models that use recent user information such as number of checks and cumulative dollar amount recently written by the user, historical data on returned checks presented to the system, etc. Additionally, positive information on the consumer or transaction may be used to authorize a transaction that otherwise would be deemed high risk. The risk management technologies may also use artificial intelligence when interpreting the user information.

With the amount of information gathered on Internet check transactions, processes normally confined to voice referral transactions may now be made available for Internet transactions, including the commercially known A 1 model, credit score access via name and address, and others. These transactions and analyses may be executed in real time, to provide the retailer and consumer an online response, or through batch processing, based on the vendor's preference or otherwise.

If the service provider approved upon selection of a check payment option, an ACH funds transfer may be initiated, or a paper draft may be generated, based on the retailer's requirements or whether the transaction can be "ACHed". If the transaction vendor 106 (retailer) has subscribed to a settlement service from the service provider and the transaction can be processed through ACH, then an ACH fund transfer may be initiated. This may be done by transmitting the transaction to an ACH provider in an offline batch or other mode. Funds from ACH transactions are usually made available within two banking days, depending on the transacting bank's ability to post the funds.

For vendors (merchants or subscribers) under a payment warranty program such as that offered by Equifax Inc., all ACH funds, even from returned items, are available within the two banking day timeframe. The warranty program is a service where a service provider guarantees that a check transaction, once properly approved by the service provider, will not be returned.

For vendors participating under a self-risk program, collection functions may be provided by an outside service or the vendors themselves. The self-risk program is a program where the transaction vendor 106 bears the risk of a return check. A check may be returned for many different reasons, even after it has been approved by the service provider of secure network transactions.

If the consumer alternatively wishes to pay by credit card, then the transaction is routed to transaction card server 140 for processing or to the vendor's designated card processor. If the transaction vendor 106 offers a private label card, then the point of sale (POS) promotion server 128 may be used. Alternately, the transaction card server 140 may also be used when a private label card is selected as the payment method. A private label card is a credit card offered by a merchant, such as Sears™ card or Shell™ card.

The invention offers an increased customer base/transaction volume for electronic commerce, and permits a unified provider of payment solutions for vendors for all of their transactions, whether generated through store outlet, virtual storefront (Internet), telephone, mail, fax order, or others.

The payment architecture of the invention also promotes increased purchaser satisfaction and loyalty. Many retailers are expanding their businesses by creating Internet storefronts. The invention provides a complete collection of payment services, along with value-added services such as pre-approved private label credit card offers in both online and offline environments under the safe payment mechanisms offered by the invention.

Consumers operating the client device 102 may have two or more data entry options to input their authorization data elements. They can build into a prefilled payment option screen on the client device 102 the required fields for check and credit card authorization, then transmit that information to transaction server 110 or over an established direct link to authorization server 114 for each transaction. Alternatively, data entry may be automatically triggered when transaction vendor 106 notifies automation server 114 that the consumer is requesting to pay by check or card.

An authorization query box to process the payment through an electronic funds transfer may thus be included on the pay by check screen presented on the user interface

150 of client device 102. If the consumer does not agree to that type of electronic funds transfer, then the consumer may be prompted for another form of payment.

During the data entry process, the consumer may be advised and asked to acknowledge that should an attempt to execute an ACH transaction fail, a signatureless paper draft will be created and processed through normal banking channels. The consumer may also be notified of applicable service fees associated with any returned items (electronic or paper draft). Delivery of the transaction may be through a true web transaction with the transaction server 110 serving as a web server. The transaction server 110 provides security through transaction encryption.

In conjunction with the invention, indicators may be established to identify merchants who have a compatible capability process transactions over the Internet or otherwise. A new service restriction (for example "web") may be added on associated servers and on one or more files or client device 102. A new code (for example "I") may be used within the inquiry log file (ILF) and OASys log file, to indicate remote transactions processed and paid through the Internet or other channels. ILF is a file that logs all check transactions. OASys is a maintenance application that assists access of log files.

Returning to the authentication process of the invention, a front-end authentication engine may authenticate the consumer to confirm his identity. For authentication, the consumer may be prompted to create a password that is tied to the login ID, which may be stored in the consumer database 122. A link from the check authorization server 124 to the authentication server 114 may be established. In future return visits, when the consumer arrives at the virtual storefront of transaction vendor 106, the consumer will be prompted to enter a login/password, the transaction server 110 will validate the login/password by retrieving the consumer's login information from the consumer database 122. Alternatively, the transaction vendor will pass the transaction to the authentication engine, and the consumer will be prompted to enter a login/password.

The login/password also index the consumer database 122 and may be used to reference other consumer records. For instance, the login/password may be used to obtain consumer records such as driver license information and full MICR data used to populate the authorization request for processing.

The authentication server 114 may have processes responsible for removing aged records (active and inactive), deleting fraudulent data, and removing records associated with uncollected checks.

The transaction server 110 may have additional processes. One process may handle consumer support for declined transactions based upon certainty scores or the inability to authenticate the consumer. Other process may prevent fraudulent check writers from reregistering and obtaining new certainty scores according to the invention.

The transaction server 110 may develop and maintain the consumer database 122 to store the various elements required to process associated transaction information such as check warranty, check verification, self-risk, ACH settlement, paper draft deposit, and POS promotion transactions. Collections information may be made available for ACH and paper draft returns. A flag may indicate if the information in the consumer database 122 was obtained directly from the consumer, or retrieved from other databases. Records may be purged from the consumer database 122 after a predetermined time to keep the consumer information up to date. The purging of records from the consumer database 122 may coincide with the purging of aged records on the authentication server 114, which would require previously authenticated consumers to re-authenticate on the next transaction.

In addition to the consumer database 122, the transaction server 110 may house or interface to an auxiliary log file 152 containing transaction data that will enable returned items to match consumer information. The key data used to match a returned ACH transaction or paper draft to the log file 152 to obtain the consumer data may include transaction data such as ACH full MICR number, amount, check date, ACH tracking number (if item was ACHed), and merchant ID.

The log file 152 may contain at least the following information:

Table 1

- Consumer Name
- Gender (consumer entered, internal source or implied)
- Consumer's Full Address
- Address for ACRO database (e.g. obtained through Equifax, Inc.)
- Email address
- Consumer's Phone Number

- Company Name, if company check
- Company Full Address
- Company Phone Number
- Merchant Number
- Check Amount Type (personal/company)
- Check Amount
- Driver's License
- State of Issuance
- Date of Birth
- Social Security Number
- Full MICR
- Check Number
- ACHable Full MICR (if different than full MICR)
- ACH tracking number

The consumer database 122 may contain at least the following information:

Table 2

- Consumer Name
- Consumer's Full Address
- Shipping address
- Alternate ship to frequency indicator
- Address from ACRO database (e.g. obtained through Equifax, Inc.)
- Email address
- Consumer's Phone Number
- Company Name
- Company Full Address
- Company Phone Number
- Driver's License
- State of Issuance
- Date of Birth
- Social Security Number
- Bridge data to eliminate the necessity of the Bridge file

- Positive File/VIP attributes
- AI Model Score
- Activity (velocity)
- Gender (consumer entered, internal source or implied)
- Check Account Type (personal/company)
- Last Used Check Number
- Full MICR
- ACHable Full
- NOC Account Number
- Preferred Credit Card Number/expiration
- Certainty Score
- Login/Password
- Challenge Question/Answer (may be based on conjunction with digital certificate logic)

In terms of transaction response, the authorization message generated by transaction server 110 may be based upon a direct link field specification, four fields: Ship to Indicator, Company Name, Company Address, Company phone, consumer login and password.

Table 3

Field	Description	Field Size
1	MESSAGE LENGTH**	2
2	TRANSACTION ID	4
3	SEQUENCE NUMBER	6
4	STATION NUMBER	10
5	TRANSACTION TYPE	2
6	CONSUMER LOGIN	7
7	CONSUMER PASSWORD	7
8	STATE CODES AND ID TYPE	2
9	ID	33
10	CHECK NUMBER DELIMITER	1
11	CHECK SEQUENCE NUMBER	6
12	DATE OF BIRTH	8

13	AMOUNT	7
14	EXPANSION ID	4
15	FULL MICR LINE	26
16	SWIPE INDICATOR	1
17	CHECK TYPE	1
18	ADDITIONAL DATA	20
19	NAME 1	55
20	NAME 2	55
21	ADDRESS	40
22	CITY	20
23	STATE	2
24	ZIP CODE	9
25	HOME TELEPHONE NUMBER	10
26	SOCIAL SECURITY NUMBER	9
27	COMPANY NAME	55
28	COMPANY ADDRESS	55
29	COMPANY PHONE	10
30	SHIP TO INDICATOR	1
31	RECORD DELIMITER	1

In terms of decision engines employed by the transaction server 110, a certainty score of 0-100 or other scales may be used to determine whether the consumer will be permitted to use a selected payment option. The consumer's score may be compared to the threshold selected by transaction vendor 106 or otherwise. When the transaction server 110 processes a payment event as a warranted payment, the transaction server 110 may set the threshold for warranty accounts. Self-risk accounts may be set to self-determined thresholds for individual vendors. Separate scores may be set for check and card service under the same vendor.

The transaction vendor 106 or the service provider may perform, on an ongoing basis, analysis, validation, and adjustment of score thresholds. Such adaptations may ensure that thresholds are set properly in order to detect not only frauds, but also to avoid the system declining desirable consumers. The system may report periodically to transaction vendor 106 the total number of turndowns due to scores not meeting retailer's requirements. The transaction vendor 106 or the service provider may impose a turndown cap for each type of transaction. If the number of the turndowns reaches the turndown cap, the system may notify the transaction vendor 106 or may suspend future operations for that type of transactions. In an alternate embodiment, the certainty score may be incorporated into a transaction model used to determine whether the transaction should be accepted.

The transaction server 110 may also submit inquiries to a third party or internally operated database that houses negative address information. The information housed in this database may consist of known addresses associated with fraudulent activity, addresses associated with prison, correctional institution, mail drops, etc. The address information may be processed by a standardization routine. This information may be compared to the "bill to" and "ship to" address fields included in the transaction or from consumer database 122. If a match is made, additional risk parameters may be enabled or thresholds adjusted.

Because address standardization and matching logic routines may not be 100% accurate, it is preferable not to generate a turndown based solely on an address that has been recognized as negative. Instead, this factor may incorporated in an AI or other model used in conjunction with other factors to make the appropriate decision.

The transaction server 110 may in some cases, prior to ACH origination, identify non-ACHable items or identify them after they had been returned by an origination depository financial institution (ODFI). The transaction server 110 processes these non-ACHable items using commercial check drafting software modules. The transaction server 110 prints the paper drafts in-house, and submits these items for deposit using traditional methods. There are commercially available software packages available for such functions, for example, Intellacheck™, Troy™, Draft Creator™, Chekfaxx™ and others.

In some implementations of the invention, transaction vendor 106 may opt to integrate check drafting into an order fulfillment process, using the secure payment process of the invention for authorization only. Presently, check drafts may not be electronically represented per National Automated Clearing House Association (NACHA) regulation. Therefore, various adaptations may be made to identify drafts and exclude them from electronic re-presentment, for instance by tagging them for manual redeposit. However a variety of check processing techniques are possible and extensible using the invention.

Fig. 2 illustrates a flowchart of a process that may be used according to the invention to service ACH transaction origination and returns. In step 202, processing begins. In step 204, each consumer is set up in consumer database 122 with an associated bank account or other financial account number designated for ACH debits and credits. For merchants who are warranty clients, all funds may be credited to the client's account within two banking days. For merchants who are self-risk clients, funds from cleared items may be credited in two banking days.

In step 206, ACH transactions are formatted into the ACH record format known in the industry, using the standard entry class code. In step 208, a unique ACH tracking number may be generated and inserted into the record of consumer database 122. In step 210, the name field may be filled with the consumer name, which is an optional field by NACHA standards, but preferably used in the invention to help ensure the ACH is processed, along with other required fields. In step 212, the full MICR may be run against the consumer database 122 to determine if an NOC (notice of change) of MICR number was received from the financial institution on a previous ACH.

In Step 214, the full MICR may be run through the TEPS system to convert to the correct MICR number. The TEPS system possesses files with negative information collected from different financial institutions. In step 216, the full MICR may be run against a conversion package, such as the commercially available Thomson Epic Ware™ System. Epic Ware™ may change or convert the full MICR to the one that the financial institution needs to perform the ACH.

In step 218, the ACH transaction file may be originated through ODFI or directly through the Federal Reserve. Auditing may be done on this process, from file creation through receipt by ODFI/Fed, and finally through settlement. Settlement/reconciliation reports may be generated daily or at other intervals. In step 220, the consumer database 122 may be updated with any NOC records. An NOC is sent to the originator when the full MICR sent on the ACH is different than the full MICR the bank uses to do the ACH.

In step 222, the invention may expand Claims system, ERMS/CUBS, Collections' Derogatory Information File System (DIFS), PathWays self-risk or any other files or information that carry return codes to allow a 2-byte ACH return code, or other desired format. When the ACH returns file is received, step 224, each item is matched to an ACH log file to retrieve all consumer information needed to create a Claims record, add to the Claims system, then to ERMS/CUBS if self-risk and transaction server 110 or other parties are doing collections. The Claims system is a system for handling returned checks and collections.

In step 226, the system may generate Internet and US mail collection letters for those ACH transactions that were returned (Warranty Collections and ERMS). Criteria to determine which letters are sent, and via which medium, may include several variables, such as total transaction amount and certainty score. In step 228, this type of processing ends.

Several ACH return codes may be defined in the system as administrative return codes. These returns preferably do not feed DIFS, and preferably do not generate the normal collection letters. The ability to designate special processing, such as creating paper drafts for deposit, may be included in implementations of the invention.

Re-presentment parameters may be defined to determine whether the payment instrument is eligible for re-presentment and the timing of the re-presentment and may include such variables as ACH reason code, dollar amount, ACH origination date, and date of return. Timing of the re-presentment may be managed and adjusted so that the item is represented on a date or day of the month most likely to clear. In addition, the number of representations may be tracked, so that an item is not re-presented more than a predetermined number of times (e.g. two).

Warranty Collections and CUBS systems may be flagged when an item is in redeposit. If the item goes out on redeposit and does not come back as a return within a predetermined number of days, then the item may be marked as paid. At that time, any service fee ACH that was authorized by the consumer may be originated. Within a predetermined number of days, ACH may clear the service fee and the fee may be posted as paid.

If a return is received late on either the check amount or service fee, the item may be reversed. However, if the RDFI (receiving financial institution) sends it back later than allowed by NACHA guidelines, then the institution may be responsible. An exception report may be created to show these exceptions.

The authorization server 114 or other resource may also present a user interface to allow transaction managers to apply debit/credits manually. That manual adjustment interface may preferably have a highly secure, restricted access, with audit reports to show activity by user. This interface may be preferably used where an ACH error needs to be corrected. Adjustment date, dollar amount, full MICR number (credit), full MICR number (debit), and a comment line to enter reason for adjustment may be included in the input.

For all ACH items, the transaction server 110 may permit settlement with the transaction vendor 106 within 2 banking days of the transaction being processed. Transaction vendors 106 operating on a warranty basis may receive all funds within that timeframe even if the funds do not clear. Paper drafts created for a non-ACHable warranty items may be settled in the same timeframe.

The generation of timely reports reflecting actual settlement information is a significant element of transaction processing according to the invention. To assist vendors with reconciliation, reporting mechanisms may be preferably configured to allow vendors to accumulate data over a requested time period. For instance, the system may generate check warranty reports that contain daily settlement information showing items that were sent out for ACH each banking day and non-ACHable items that we submitted via paper draft for settlement.

For transaction vendors 106 operating on a non-warranty basis, a daily settlement report may be generated that shows what was submitted as an ACH and what vas submitted via paper draft. Reporting statements, which depict returned items, may preferably include original transaction date, date submitted, return date and return code. Reports may be accessible through the Internet or other communications channels, as well as by paper delivery.

In another regard, an audit report may be generated for the purpose of reconciling chargebacks (warranty returned items) to funds debited from any settlement account accessed by the transaction server 110. An operator of a transaction server 110 may establish a settlement bank account to keep warranty-clients “whole” through the settlement process, i.e., the warranty returned items are charged against the settlement bank account and not charged to the warranty clients. A third party ACH originator/provider may front all funds to the warranty client, and debit all returns against the settlement account. This type of reconciliation is particularly helpful if a third party handles the ACH origination and settlement functions, since they will debit accounts of the operator of the transaction server 110 for all warranty returns.

An automated claims data entry system may be employed to allow a high volume of claims to be processed efficiently. Commercial solutions, such as Elec Check™by Equifax Check Solutions, may be used. All ACH returns may be used to trigger an update to claims and the negative file without human intervention. The ACH returns need to be matched against the consumer database 122 to pull additional consumer information needed for collections. ACH return codes may be incorporated into data fields or resources such as Claims, ERMS (CUBS), IXFS, IVR, and Collections. Collection letters (e.g. electronic mail and US Mail) may be generated incorporating ACH codes into the process.

Warranty and ERMS collections letters for items processed through the Internet may require modifications. The modifications may include the Internet and ACH return-related indications or verbiage. Collections letters may be sent via electronic email or US mail. It is preferable that an electronic mail be sent first and followed by a standard US mail if no response from the consumer is obtained. It is preferable that if a consumer receives information about their claim status over the Internet. If the money is owed, a link with Western Union™ may be established for payment arrangements mirroring the Quick Collect™ or other programs.

The invention provides for delivery of current consumer disclosure information. Declined or delayed consumers may be able to call into an operator of transaction server 110 and access an Interactive Voice Response (IVR) or other system. Where applicable, return codes and other identifiers may be assigned to distinguish Internet transactions. For example, a code may be used to identity those where the consumer's certainty score falls below a vendor's assigned threshold. To provide true Internet disclosures, IVR and other service applications may be integrated into a Web portal site by the use of Periphonics' PeriWeb™ or other products. The invention may incorporate the ability to automatically generate email disclosing to the consumer the events associated with a particular transaction.

Now turning to Fig. 3, which describes a user process 300 according on one embodiment of the present invention. The present invention is particularly useful to assist merchants to handle non-cash payment consumer transactions in a secure way. A system according to the present invention can handle a consumer shopping through the Internet, placing an order through a telephone, or purchasing in person at a storefront. The user process 300 described herein is based on a consumer shopping through the Internet, but people skilled in the art will appreciate the process is equally applicable for other situation described above.

The consumer shops on line by visiting a virtual storefront through a web site, step 310. After selecting products, the consumer proceeds to check out, step 320, and selects the appropriate payment type. The web site, or the virtual store, redirects the consumer to the authentication process. The authentication process checks whether the consumer has been authenticated, step 330. The authentication process verifies the consumer's identity. The identification process is preferably handled by an outside vendor, such as Equifax™, who is specialized in authentication process. If the consumer has not been authenticated, then he is referred to the authentication process, step 340. After the consumer goes through the authentication, if the authentication is successful, step 350, he proceeds to complete the payment method, step 370. If the authentication fails, his purchase is declined.

If the consumer has been authenticated before, either by this merchant or a different merchant, the consumer would have been assigned an identification code (ID) and a password. In an alternate embodiment, where a less complex authentication process is used, the system may not issue a login ID nor a password to the consumer. The consumer would provide his ID and the password, step 360. After he provides his ID and his password, the system retrieves his record from a database. This record has consumer's information such as consumer's certainty score. The system then prompts him to complete payment, step 370. The present invention support equally on-line check payment, debit card payment, credit card payment, or other form of on-line or off-line payment method.

After the consumer completes his payment, and the system starts a payment process, step 380. The payment process is also preferably handledby an outside vendor who has expertise in handling on-line transactions. A merchant can easily set up a virtual storefront by subcontracting the authentications and payment services from an outside service provider and handling the product ordering process internally.

After the payment method is handled properly, the merchant is ready to ship the merchandise to the consumer.

Fig. 4 illustrates an authentication process 400 used in one embodiment of the present invention. The authentication process prompts and receives the consumer's identification information, step 410. The identification can be consumer's name, address, driver license number, etc. The authentication process then checks the information received against some database generally available for this purpose, step 420.

The authentication process may be a multi-stage authentication process, where the first stage employs a commonly accessible "wallet-type" information, such as name, address, telephone number, driver license number, social security number, etc. and the second stage relies on information not easily obtainable, such as credit related information.

For a multi-stage authentication process, steps 410 and 420 are repeated as necessary. The format employed to gather information may be "question and answer" or multiple-choice formats.

After the information is received, either through a simple authentication process or a multi-stage process, the authentication process generates a certainty score, step 440, based on the information provided by the user. The certainty score may be calculated using different algorithms. The algorithms take into consideration the level of acceptable risk and the correctness of the information provided by the consumer.

If the certainty score is high enough, step 450, then a user ID and a password are generated, step 460. This user ID and password may be used in subsequent access to the same virtual store or to other stores that employs the same system. The system also creates a record for the consumer, step 470. The authentication process then returns the consumer and his information to the calling user process.

If the certainty score is low, which means that the system cannot verify the identity of the consumer confidently, the authentication is denied, step 480. The authentication process may provide instruction on how to learn more about his situation, such as providing a toll free telephone number for the customer support. The authentication process may also transfer the consumer to merchant's consumer service desk.

Fig. 5 illustrates a payment process 500 according to one embodiment of the present invention. The payment process receives information about the consumer, step 510. The payment process determines whether a payment from the consumer should be accepted or declined. The consumer may have been properly authenticated with a high certainty score by the authentication process, but nevertheless has his payment declined. Among the factors that cause a payment be declined are the consumer has unpaid returned checks on file, the consumer has reached check acceptance limits, the consumer is a new user and has written many high amount checks, the consumer started a unusual spending pattern, the consumer's check may has been reported stolen, etc. The payment process employs artificial intelligent algorithms based on different risk factors.

The check authorization process first checks the consumer's identification numbers against validation files. The check authorization process checks the consumer's information against a negative file, step 520.

After checking the negative file, the system proceeds to retrieve the consumer's record from transactional and consumer databases, step 530. The system may analyze the information from the consumer' record against a risk model to determine whether the payment should be accepted, step 540. The risk model may employ different algorithms that consider different risk factors. During the payment process, if the system detects any problem, the system sets a flag indicating the problem. If the consumer or transaction has a positive attribute, the flag may be overridden and the payment approved.

At the end of the process, the system checks whether any flag was set, step 550. If no flag was set, then the payment is approved, step 560, otherwise the payment is denied, step 570. If the payment is approved and the merchant has subscribed to a payment settlement service from the service provider, then the payment information is forwarded to a settlement process. The payment settlement process as described above prepares payment information in a proper format and sends it for processing by a centralized clearing house. The funds will be credited to the merchant's account automatically.

The foregoing description of the invention is illustrative, and variations in configuration and implementation will occur to persons skilled in the art. For instance, while the invention has generally been described with respect to real time processing of individual transaction events, different events or parts of events may be grouped for batch processing when appropriate.

Similarly, while the invention has been described as taking place within a single banking system or currency, currency conversion and other international or inter-monetary processing may be incorporated. Different computing and other elements, which may have been described as separate, could be combined, and different computing and other elements illustrated as singular could be distributed amongst different platforms or resources. The scope of the invention is accordingly intended to be limited only by the following claims.

What is claimed is:

1. A method of managing electronic transactions between a client and a vendor over a network, comprising the steps of:

a. receiving an authorization request from the vendor for a transaction requested by the client;

b. interpreting payment information within the authorization request to associate a payment type with the transaction; and

c. performing an authentication process against the authorization request to determine if the payment type is validated for the transaction request; and

d. generating a response to the authorization request.

2. The method of claim 1, wherein the payment type comprises at least one of a check payment process, a debit payment process and a credit process.

3. The method of claim 1, wherein the step (c) of performing an authentication process comprises a step (e) of determining whether an account may be processed according to Automated Clearing House standards.

4. The method of claim 3, further comprising a step of (f) transitioning the transaction to a different payment process when the account may not be processed according to Automated Clearing House standards.

5. The method of claim 1, further comprising a step of (g) presenting a promotional option to the client at the time of payment processing.

6. The method of claim 1, wherein the step (c) of performing an authentication process comprises a step of (h) invoking at least one of a set of selectable authentication engines.

7. The method of claim 1, wherein the transaction comprises a network purchase transaction.

8. The method of claim 7, wherein the network purchase transaction comprises a transaction over the Internet.

9. The method of claim 7, wherein the network purchase transaction comprises a telephonic transaction.

10. The method of claim 1, wherein the step (d) of generating a response comprises a step i) of indicating to the client that payment processing will proceed using a signatureless paper draft.

11. A system for managing electronic transactions between a client and a vendor over a network, comprising:

a first interface for receiving an authorization request from the vendor for a transaction requested by the client;

a processor, communicating with the first interface, the processor interpreting payment information within the authorization request to associate a payment type with the transaction;

a second interface to an authentication process against the authorization request to determine if the payment type is validated for the transaction request; and

a third interface to output a response to the authorization request.

12. The system of claim 11, wherein the payment type comprises at least one of a check payment process, a debit payment process and a credit process.

13. The system of claim 11, wherein the authentication process comprises determining whether an account may be processed according to Automated Clearing House standards.

14. The system of claim 13, wherein the authentication process comprises transitioning the transaction to a different payment process when the account may not be processed according to Automated Clearing House standards.

15. The system of claim 11, wherein a promotional option is presented to the client via the third interface at the time of payment processing.

16. The system of claim 15, wherein the authentication process comprises invoking at least one of a set of selectable authentication engines.

17. The system of claim 11, wherein the transaction comprises a network purchase transaction.

18. The system of claim 17, wherein the network purchase transaction comprises a transaction over the Internet.

19. The system of claim 17, wherein the network purchase transaction comprises a telephonic transaction.

20. The system of claim 11, wherein the response presented to the client comprises an indication that payment processing will proceed using a signatureless paper draft.

21. A method for managing a plurality of electronic transactions between a consumer and a vendor over an network, the method comprising:

establishing a threshold score for each given transaction;

receiving a selection of an electronic transaction from the consumer;

obtaining input from the consumer;

creating an overall certainty score; and

comparing the overall certainty score with the threshold score of the selected electronic transaction.

22. The method of claim 21, wherein the creating step further comprises

comparing the input with data from a database; and

scoring the input using a scoring algorithm.

23. The method of claim 22, wherein the database is an external database having consumer credit information.

24. The method of claim 21 further comprising authenticating the consumer through a two-step authentication process, wherein a second step authentication uses information from a credit database.

25. The method of claim 21 further comprising

switching to an alternate electronic transaction, if the overall certainty score is less than the threshold of the selected electronic transaction.

26. The method of claim 21 further comprising

instructing the consumer on how to obtain information regarding the selected electronic transaction, if the overall score for the consumer is less than the threshold score.

27. The method of claim 21 further comprising

formatting the input received from the consumer into a record ready for automatic clearing house processing.

28. A method for handling non-cash payment transactions between a consumer and a vendor over a network, the method comprising:

receiving a user identification code and a password from the consumer;

retrieving a consumer record, the consumer record having consumer information;

prompting for a payment method;

determining whether to accept the payment method using the consumer information in a risk model, wherein the risk model uses information retrieved from a credit database.

29. The method of claim 28 further comprising authenticating the consumer through a multi-step authentication process and assigning an identification code and a password to the consumer.

30. The method of claim 29, wherein the multi-step authentication process employs a multiple-choice question format and uses information from the credit database.

31. The method of claim 29 further comprising assigning a certainty score to the consumer, wherein the certainty score is based on the correctness of information provided by the consumer.

32. The method of claim 28 further comprising checking a negative file, wherein the negative file containing information selected from a group consisting of a list of stolen identities, a list of closed bank accounts, and a list of bad checks.

33. The method of claim 28, wherein the risk model further uses information on the consumer's recent spending pattern.

34. The method of claim 28, wherein the risk model further users historical data on returned checks.

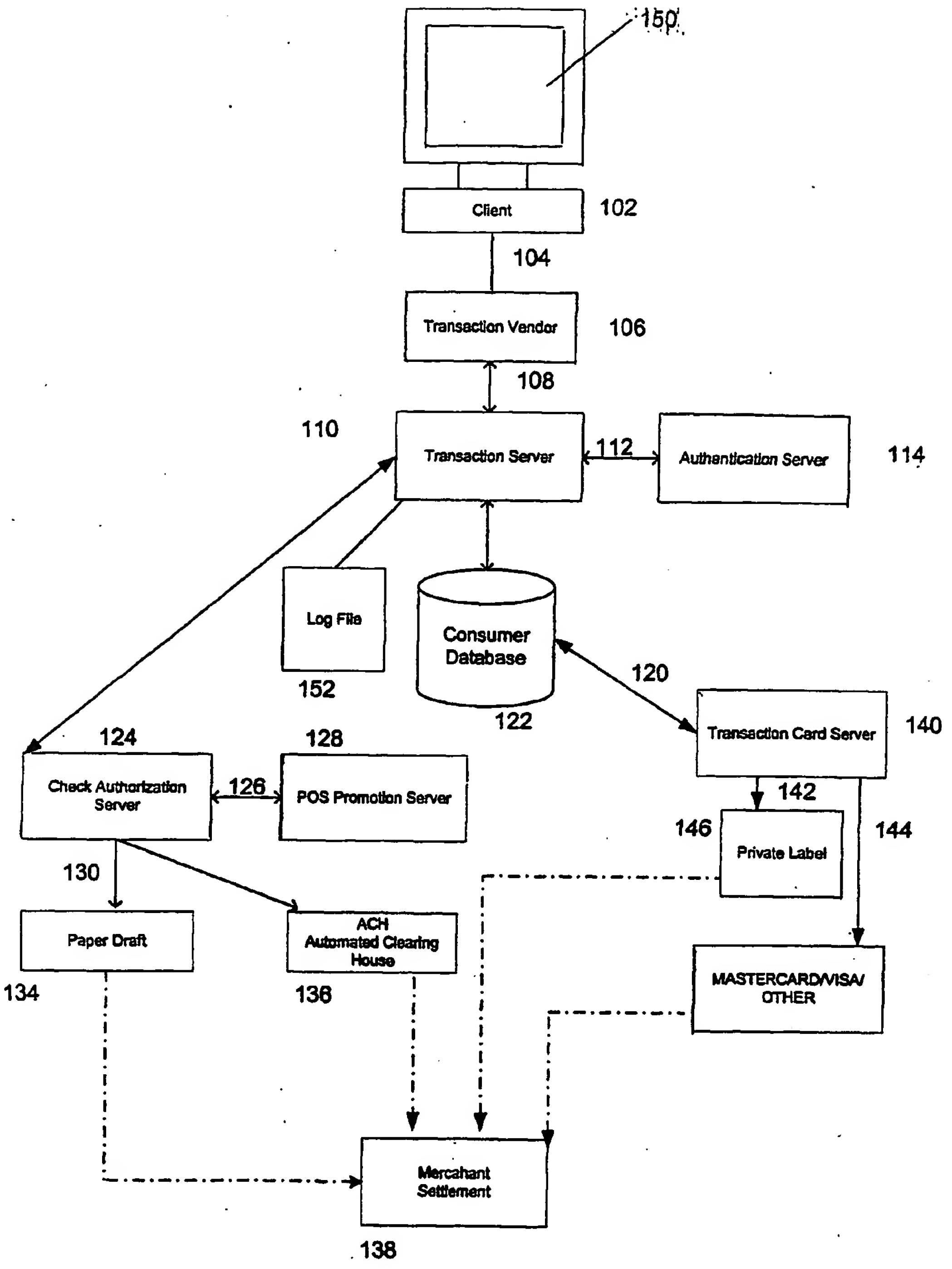
150
Client
102
104
Transaction Vendor
106
108
110
Transaction Server
112
Authentication Server
114
Log File
152
Consumer Database
122
120
Transaction Card Server
140
124
Check Authorization Server
126
128
POS Promotion Server
142
146
Private Label
144
130
Paper Draft
134
ACH Automated Clearing House
136
MASTERCARD/VISA/ OTHER
Mercahant Settlement
138

Figure 1

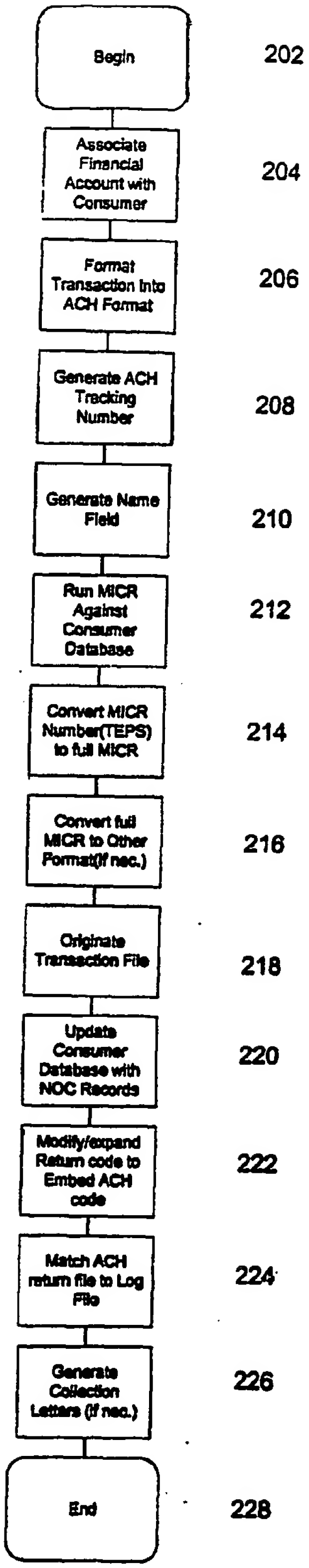
Begin
202
Associate Financial Account with Consumer
204
Format Transaction into ACH Format
206
Generate ACH Tracking Number
208
Generate Name Field
210
Run MICR Against Consumer Database
212
Convert MICR Number(TEPS) to full MICR
214
Convert full MICR to Other Format(if nec.)
216
Originate Transaction File
218
Update Consumer Database with NOC Records
220
Modify/expand Return code to Embed ACH code
222
Match ACH return file to Log File
224
Generate Collection Letters (if nec.)
226
End
228

Figure 2

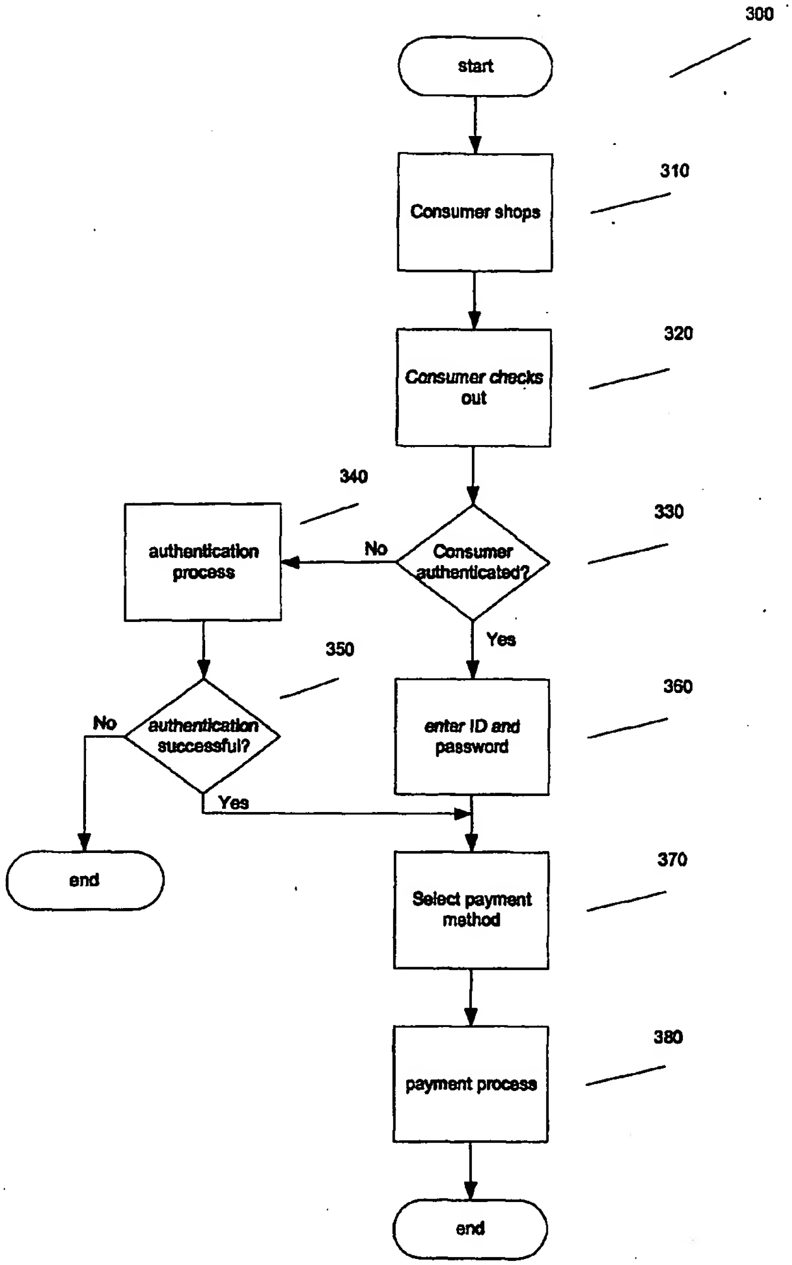
300
start
Consumer shops
310
Consumer checks out
320
Consumer authenticated?
330
No
authentication process
340
Yes
enter ID and password
360
authentication successful?
350
No
Yes
end
Select payment method
370
payment process
380
end

Fig. 3

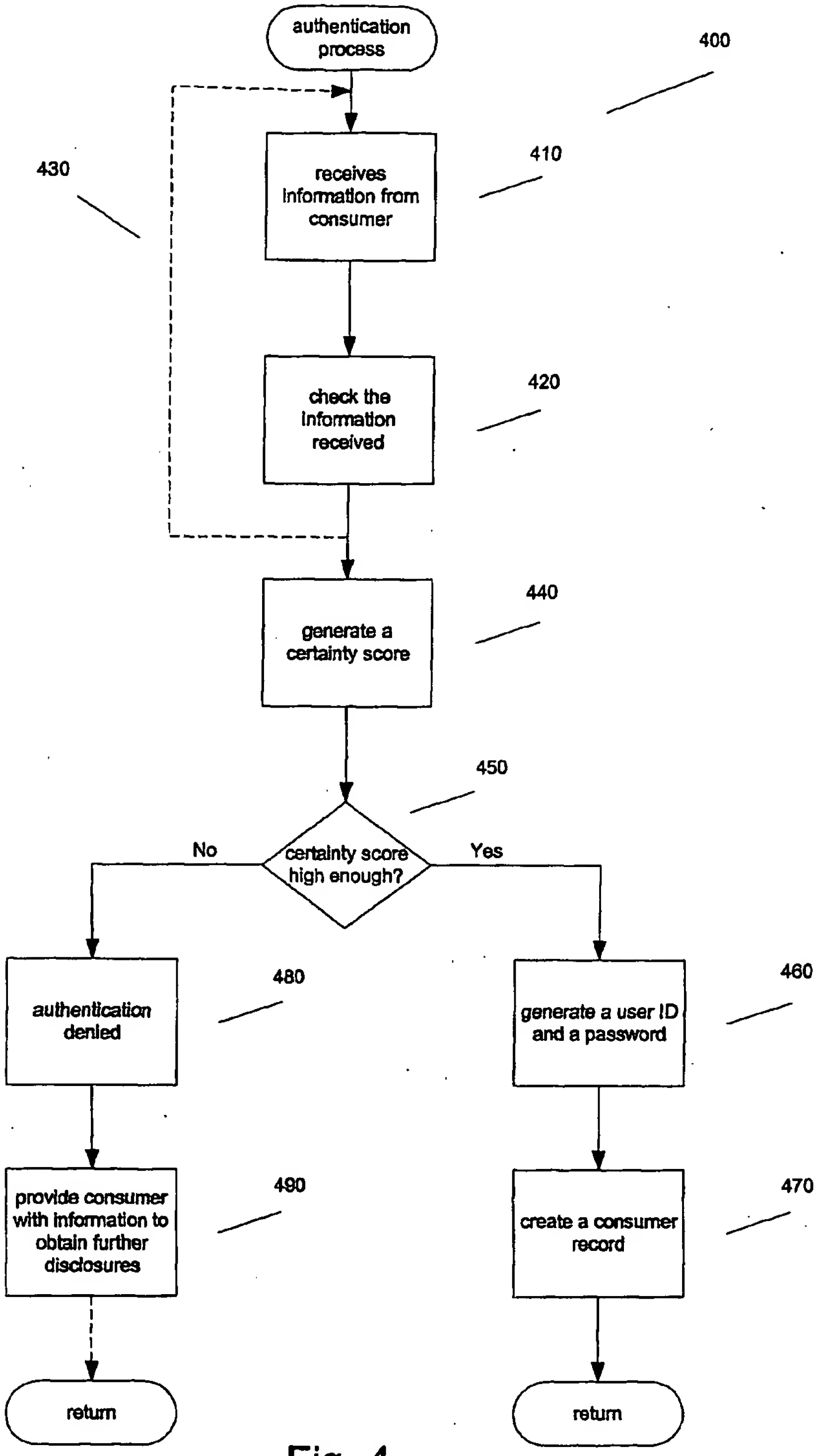
authentication process
400
430
receives information from consumer
410
check the information received
420
generate a certainty score
440
certainty score high enough?
450
No
Yes
authentication denied
480
generate a user ID and a password
460
provide consumer with information to obtain further disclosures
490
create a consumer record
470
return
return

Fig. 4

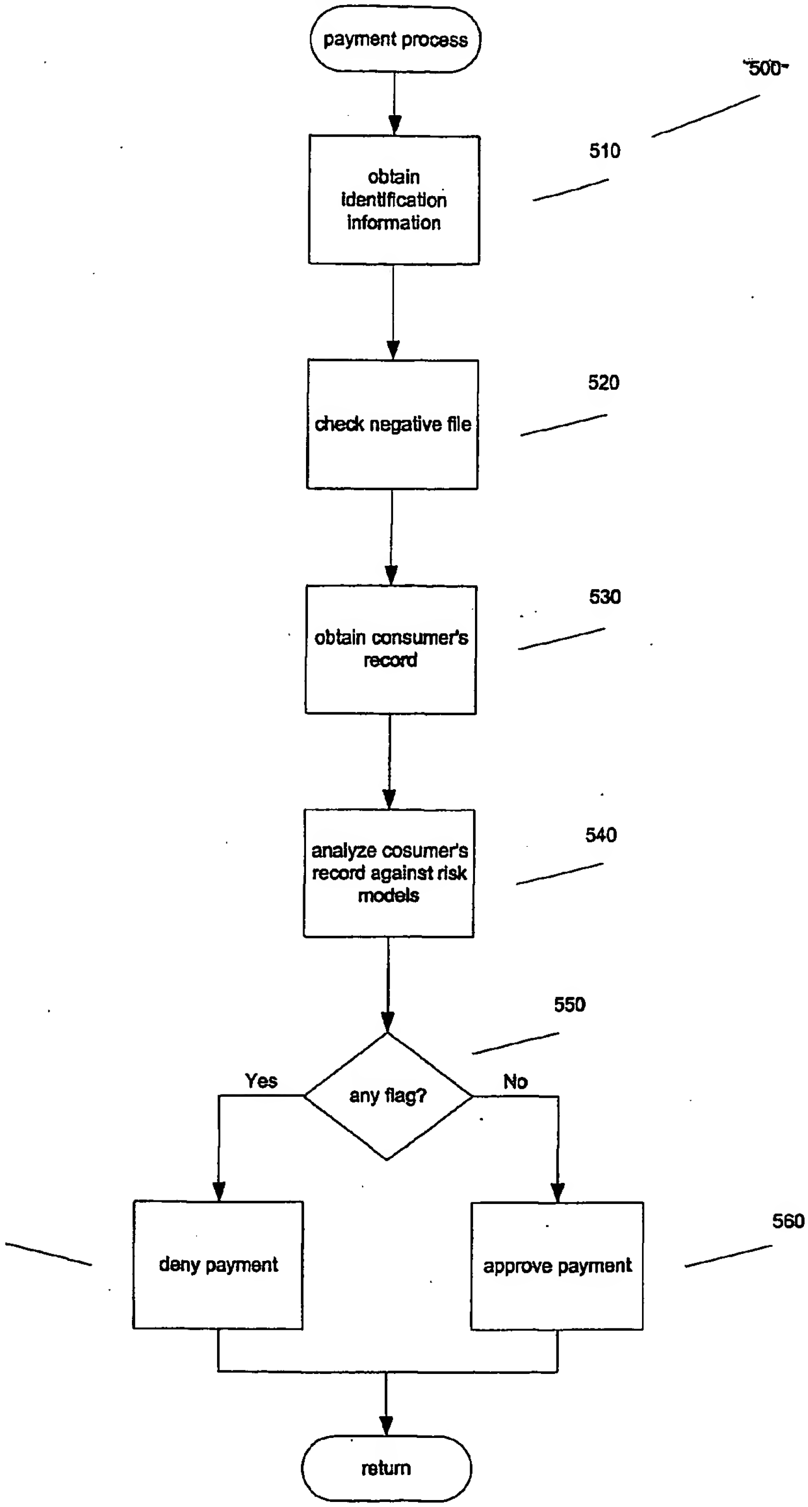
payment process
500
510
obtain identification information
520
check negative file
530
obtain consumer's record
540
analyze cosumer's record against risk models
550
any flag?
Yes
No
570
deny payment
560
approve payment
return

Fig. 5